BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-321

3 AUGUST 2011

Communications and Information

AUTHENTICATION OF AIR FORCE RECORDS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **http://www.e-publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6PPF

Certified by: SAF/A6PP
(Mr. Albert Bodnar)

Supersedes: AFI33-321, 27 July 2006

Pages: 9

This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management*. It provides a definition for Air Force records and provides authentication instructions. This publication applies to all Air Force organizations, civilian and military personnel, Air National Guard (ANG), Air Force Reserve Command (AFRC), and contractor personnel, regardless of the information media transmitted or received. This publication sets forth policies for personnel to observe the prohibition in paragraph 5.2. Failure to observe paragraph 5.2 by military personnel is a violation of Article 92 of the Uniform Code of Military Justice (UCMJ) and may also subject them to administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws involving the willful and unlawful destruction of federal records. In addition to criminal and civil sanctions under applicable laws, civilian employees are subject to administrative discipline for violating paragraph 5.2, while contractor personnel are subject to action under the terms of their contract or otherwise by their employer for violation of paragraph 5.2. Send recommended changes or comments to Secretary of the Air Force, Air Force Records Office (SAF/A6PPF), 1401 Wilson Blvd, Suite 600, Rosslyn VA 22209 through appropriate channels, using AF Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records,* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. See **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. This instruction defines records, authentication authority, methods to authenticate records, and misuse of authentication authority or methods.

1. Purpose. Records serve a vital role in documenting the Air Force mission and provide evidence and accountability of our organization, function, policy, and procedures to the public, congress, and the Department of Defense (DoD). This publication defines what establishes an individual's authority to authenticate records and prescribes the accepted methodologies for authenticating Air Force records.

2. Records Defined.

2.1. **Definition.** Records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included. Records are further defined in AFMAN 33-363, Management of Records.

2.1.1. Final records are those that have been signed, officially released, and shall not be altered, see AFMAN 33-363.

2.1.2. Records may have a permanent or temporary value to an organization.

2.1.2.1. Permanent records are those that have been determined by the Archivist of the United States to have enduring value as documentary evidence of the organization and functions of the Air Force. Permanent records are accessioned to the National Archives for preservation in accordance with the Air Force Records Disposition Schedule (RDS). Life cycles of records are annotated in the Air Force RDS maintained in the Air Force Records Information Management System (AFRIMS).

2.1.2.2. Temporary records are those determined by the Archivist of the United States to have insufficient value to warrant preservation. Temporary records are disposable after a fixed period of time in accordance with the Air Force RDS. Life cycles of records are annotated in the Air Force RDS maintained in AFRIMS.

2.1.3. Records are media neutral, meaning that records can be electronic, paper, film, etc. Electronic media is the choice for use, storage, and management of Air Force records. Paper records should only be created to meet a historical and/or legal requirement.

2.1.4. Examples of different types of records include books, papers, photographs, machine-readable materials, e-mail, data in Information Technology (IT) systems, web pages, letters, memorandums, completed forms, statistical and narrative reports, graphics, photographs, negatives, audio and video recordings, microfilm, microfiche, maps, architectural, engineering, and other drawings.

3. Authentication Methods for Air Force Records.

3.1. **Authentication.** Refers to the process used to make certain the identity of a person or the integrity of the specified record information. A record is authenticated when it contains an official signature indicating the document is genuine and official. A signature may be written, stamped, or electronic. Use one of the following methods to authenticate records issued in the conduct of Air Force business:

3.1.1. Written Signature. Sign the appropriate paper-based signature block using black or dark blue ink. Do not sign for another person; official directives or statutes require the personal signature of designated persons on many types of Air Force records.

3.1.2. Signature Facsimile. A signature facsimile is an authorized copy of an individual's signature. Do not use signature facsimile to authenticate unless the records requiring signature are so numerous for that organization that the act of written authentication becomes a time-consuming task.

3.1.2.1. You may use a signature facsimile on administrative records, such as form or transmittal memorandums, see AFMAN 33-326, *Preparing Official Communications*.

3.1.2.2. Physically safeguard signature facsimile equipment such as those used to authorize the expenditure of government funds or the binding of the Air Force or the government to a course of action.

3.1.3. Electronic Signing Technologies. Refers to methods used to verify the identity of the signer and the authenticity of the data contained in the record. Electronic signatures may be accomplished by several different technologies; personal identification numbers (PIN), digital signatures, smart cards and biometrics are all approved methods of electronic signing for authenticating e-records. Information in an official Government e-mail header is a form of authentic electronic signature. Above any electronic signature block, enter "//SIGNED//" or a facsimile. This form of signing will be determined authentic for documenting e-mail and/or subject matter expert coordination when released from a Government e-mail account and when a legal requirement does not exist for either a physical or digital signature. However, a digital signature may be required on a corresponding form intended to document the same intent. In that case, the user must contact the supporting legal office for signature requirements governed by Federal statutes. That office can also advise on a case-by-case basis which venue (physical, digital, electronic signature) would be most appropriate. The most important commonly used methods are as follows:

3.1.3.1. Typed Notation. A method of signing an electronic document that (a) identify and authenticate a particular person as the source of the electronic document; and (b) indicate such person's approval of the information contained in the electronic document. The electronic signature may be embedded in the content of the record, or it may be stored separately. Formatting examples may be found in AFI 33-119, *Air Force Messaging*. (This form of signing will be determined authentic for documenting e-mail) and/or subject matter expert coordination when released from a Government e-mail account and when a legal requirement does not exist for either physical or digital signature. Typed notations may or may not be tightly linked to a

form or document, whereas digital signatures are difficult or impossible to unlink from a document.

3.1.3.2. Digital Signatures. A method of authenticating records by producing a digital signature bound to both the record and the signer's identity using cryptographic keys, operations, and protocols. Digital signatures serve to both verify a signer's identity and provide integrity for the data contained in the record.

3.1.3.2.1. A digital signature is produced by a user's computer using a PKI certificate (typically via a CAC), the record, and various cryptographic operations and protocols. Digital signatures can be produced only by someone with access to the private signing key. A digital signature is verified by a user's computer using a public verification key (publically available via trusted sources), the digital signature, the record, and various cryptographic operations and protocols. Digital signatures can be verified by anyone with access to the public verification key. The Air Force shall only rely on DoD Public Key Infrastructure (PKI) issued certificates according to AFI 33-200, *Information Assurance (IA) Management*. External PKIs are approved for use by the ASD(NII)/DoD CIO. The process for recommending approval for external PKIs is outlined in the DoD External PKI Interoperability Plan. Additional guidance can be found at the *Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records,* **http://www.archives.gov/records-mgmt/policy/pki.html**.

3.1.3.2.2. Forms managers must be consulted in advance to analyze any data collection tools that project officers have determined feasible and reliable for digital signature, vice physical signature. Additional guidance can be found in AFI33-360, *Publications and Forms Management.*

3.2. **Authentication of Electronically Signing Permanent Records.** For permanent records, organizations must ensure that the printed name of the electronic signer, as well as the date when the signature was executed, be included as part of any human readable form (such as electronic display or printout) of the electronic record. This is required so that the name of the signer will be preserved as part of the record. (See Records Management Guidance for Agencies Implementing Electronic Signature Technologies, **http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html**).

3.3. **Reproducing the Record That Has the Official Signature.** Unless stated otherwise in the applicable statute or official directive, copies of a record bearing an official signature have the same authority as the original.

3.4. **Security.** Protect classified and sensitive but unclassified (SBU) information in accordance with AFPD 33-2, *Information Assurance*; the 33-200 series publications; AFI 31-401, *Information Security Program Management*; DoD 5400.7-R_ AFMAN 33-302, *Freedom of Information Act Program;* and AFI 33-332, *Privacy Act Program.*

4. Authentication Authority.

4.1. **Authority**. An individual's right to authenticate records is granted by statute, directive, instruction, delegated authority, duty assignment, or specific position. In other words, it is the capacity in which a person acts, not grade that determines the right to authenticate records.

4.1.1. Command Capacity. The responsibility of a commander or civilian director to authenticate Air Force records, and the extent to which he or she may designate others to authenticate records, follows the principles of command and staff and the principle of delegation of duties contained in AFI 51-604, *Appointment to and Assumption of Command*.

4.1.1.1. A commander or civilian director continues to discharge command functions when temporarily absent from the place of duty (temporary duty, etc.). During absences, designated representatives continue to perform designated duties, see AFI 51-604.

4.1.2. Non-command Capacity. When a statute or other directive does not require the commander's or directors' personal signature, the deputy or vice commander is authorized to authenticate records without using the authority line. Any other subordinate, including the staff director of any headquarters below HQ USAF, who authenticates a record on behalf of a commander, must use the authority line "FOR THE COMMANDER" (or comparable official title) to indicate that he or she is acting as the Commander's authorized agent. Use of the authority line on any communication to a person or agency outside the Department of Defense is unauthorized, see AFMAN 33-326.

4.1.3. Staff and Administrative Capacity. Staff and administrative personnel can authenticate a record without the authority line when it reflects their own opinion, position, or administrative action on matters within their assigned staff or administrative functions, see AFMAN 33-326. They must use the authority line for records representing the coordinated position of the headquarters staff or for records providing instructions or authorizations.

4.1.4. Professional Capacity. Some staff officers and civilian equivalents--including doctors, chaplains, and judge advocates--sign documents in the performance of their official duties that require no authority line or further authentication. Examples include birth, death, marriage certificates, and records of certain adverse actions.

5. Misuse of Authentication Authority or Methods.

5.1. **Legal Documents and Proceedings.** This AFI does not apply to authentication of official Air Force records for admission into evidence connected with legal proceedings. Evidentiary authentication is governed by *Military Rules of Evidence 901* and AFI 51-301, *Civil Litigation*. Additionally, consult the servicing Legal Office prior to using any type of electronic signature in any disciplinary document since such procedure may be both improper and invalid.

5.2. **Destroying and Falsifying Records.** Personnel may only destroy records in accordance with the disposition instructions in the RDS located in AFRIMS. Willful and unlawful concealment, removal, mutilation, obliteration, falsification, or destruction of an Air Force record may result in criminal penalties or disciplinary actions in accordance with Title 18 U.S.C. Part 1, Chapter 101, § 2071 *Concealment, Removal, or Mutilation of Records.*

5.2.1. Title 18 U.S.C. section 2071 prohibits, among other things, the willful and unlawful destruction and falsification of Air Force records. Personnel may only lawfully

destroy Air Force scheduled records in accordance with the disposition instructions in RDS, located in AFRIMS. Unscheduled records may not be destroyed until a NARA approved disposition has been identified.

5.2.2. The willful and unlawful destruction or falsification of Air Force records by military personnel is a violation of Article 92 of the Uniform Code of Military Justice (UCMJ) and may also subject military personnel to administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

5.2.3. The willful and unlawful destruction or falsification of Air Force records by civilian employees may subject them, in addition to applicable criminal or civil sanctions for violation of related laws, to administrative disciplinary action.

5.2.4. The willful and unlawful destruction or falsification of Air Force records by contractor personnel may subject them, in addition to applicable criminal or civil sanctions for violation of related laws, to action by their employer, or otherwise in accordance with the terms of the applicable Air Force contract.

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 105-277, *Government Paperwork Elimination Act of 1998*

Title 18 U.S.C. Part 1, Chapter 101, § 2071 *Concealment, Removal, or Mutilation of Records*

Title 44 U.S.C. Chapter 31, § 3301 *Records Management by Federal Agencies*

DoD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*, 21 October 2010

AFPD 33-2, *Information Assurance*, 19 April 2007

AFPD 33-3, *Information Management*, 28 March 2006

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 33-200, *Information Assurance (IA) Management*., *Incorporating through Change 2*, 15 October 2010

AFI 33-119, *Air Force Messaging*, 24 January 2005

AFI 33-332, *Privacy Act Program*, 16 May 2011

AFI 33-360, *Publications and Forms Management*, 18 May 2006

AFI 51-301, *Civil Litigation*, 1 July 2002

AFI 51-604, *Appointment to and Assumption of Command*, *Incorporating through Change 1*, 4 April 2006

AFMAN 33-326, *Preparing Official Communications*, 15 October 2007

AFMAN 33-363, *Management of Records*, 1 March 2008

Military Rules of Evidence 901

Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records, March 11, 2005, **http://www.archives.gov/records-mgmt/policy/pki.html**

Electronic Signature in Global and National Commerce Act, 30 June 2001

Records Management Guidance for Agencies Implementing Electronic Signature Technologies, **http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html**

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

CFR—Code of Federal Regulations

DoDI—Department of Defense Instruction

IT—Information Technology

PK—Public Key

PKI—Public Key Infrastructure

PIN—Personal Identification Number

RDS—Records Disposition Schedule

U.S.C.—United States Code

Terms

Asymmetric Cryptosystem—A cryptographic system based on public/private key pair encryption and decryption. The basis of asymmetric encryption is the requirement for a pair of two keys; when one key encrypts, the other must be used to decrypt. The foundation of the public/private key pair is one key cannot be derived from the other.

Authority Line—The authority line informs readers that the person who signed the document

acted for the commander, civilian equivalent, the command section, or the headquarters. If it is used, type in uppercase, two line—spaces below the last line of the text and 4.5 inches from the left edge of the page or three spaces to the right of the page center. Use the words "FOR THE COMMANDER" unless the head of the organization has another title like commander in chief, superintendent, or commandant.

Authentication—The process used to ascertain the identity of a person or the integrity of specific record information. A record is authenticated when it contains an official signature indicating the document is genuine and official. A signature may be written, stamped, electronic or digital.

Digital Signature—A transformation of a message or document using an asymmetric cryptosystem such that a person having the initial message or document and a signer's public key can accurately determine if the transformation was created using the private key that corresponds to the signer's public key, and if the initial message or document was altered since the transformation was made.

Electronic Signature—A method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message; and indicates such person's approval of the information contained in the electronic message (*Government Paperwork Elimination Act of 1998*, section 1709(1)).

Records—Include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.

Signature Facsimile—An authorized duplication of an original signature that has the same authority as the original signature.